Fiche portant sur la campagne de Cyberespionnage baptisée *Tempting Cedar*

Description :

Selon des sources ouvertes, la société spécialisée en cybersécurité *Avast* a publié, en date du 21 Février 2018, un rapport sur la campagne de Cyberespionnage *Tempting Cedar*, qui a débuté en 2015 et a ciblé plusieurs pays à travers le monde, dont l'Algérie comme l'illustre la carte suivante.

En effet, ladite campagne se base sur le principe de l'ingénierie sociale pour diffuser son logiciel malveillant, en utilisant des faux profils *Facebook*, appartenant généralement à des femmes fictives, les cyberattaquants manipulent leurs victimes et les poussent à installer une version malveillante de l'application *Kik Messanger*. Cette application contient le logiciel espion *Tempting Cedar Spyware*, conçu pour collecter des informations telles que les contacts, les journaux d'appels, les SMS et les photos, ainsi que les informations de géolocalisation. Ces informations sont envoyées, par la suite, aux serveurs de Commande et de Contrôle (C&C).

Aussi, deux (02) autres applications sont utilisées pour diffuser ce malware. Il s'agit d'une application de gestion des données et une application journalistique. Le schéma ci-dessous illustre le mode opératoire de cette campagne de Cyberespionnage.

Indices de compromission :

Les indices de compromission pour les applications utilisées durant cette campagne de Cyberespionnage sont :

1- L'application *Kik Messanger* :
SHA-256:

•041136252FFEF074BODEBA167BD12B8977E276BAC90195B7112260AB31DDB810

•2807AB1A912FF0751D5B7C7584D3D38ACC5C46AFFE2F168EEAEE70358DC90006

•3065AD0932B1011E57961104EB96EEE241261CB26B9252B0770D05320839915F

•5259ADO4BDEA3F41B3913AA09998DB49553CE529E29C868C48DF40D5AA7157EA

•624A196B935427A82E8060876480E3OCE6867CB9604107A44F85E2DA96A7A22E

•9D1FDA875DE75DEA545D1FF84973B230412B8B4946D64FF900E9D22B065F8DCC

•B181F418F6C8C79F28B1E9179CAEFEB81BDF77315814F831AFOCF0C2507860C4

•D7A4ABA5FC2DEE270AE84EAC1DB98B7A352FB5F04FDO7C3F9E69DE6E58B4C745

•F67469C82E948628761FDFD26177884384481BA4BDBC15A53E8DF92D3F216648

•FE2996BC0C47C0626F43395EEE445D12E7CO24C1BOAA2358947B5F1D839A5868

2- L'application de gestion de données :
SHA-256:
•1DEB727CO5AA5FABF6224C0881970ACA78649A799EEB6864260DE97635FA005A

• 94ADF4C8A27722307C11F60A3CC47F9E5447179D1E0F7289F

• A411A587B4256007F0E0A3359A05A986195E76DA7334B7D

3- L'application journalistique :
SHA-256:
•58F74545D47F5DA1ECF3093F412D7D9544A33D36430AB1AF709D835A59184611

4- Liste des domaines compromis :

- chat-world.site
- chat-messenger.site
- gserv.mobi
- arab-chat.site
- onlineclub.info
- free-apps.us
- network-lab.info
- kikstore.net

<u>Mesures préventives</u> :

Afin de se prémunir de cette campagne de Cyberespionnage et de toutes les attaques de ce type, il est recommandé de :

- **Sensibiliser le personnel sur les risques liés à l'utilisation des réseaux sociaux ;**
- **Utiliser une solution antivirale mise à jour quotidiennement pour la détection et la suppression des malwares ;**
- **Veiller à l'application des mises à jour des systèmes d'exploitations ;**
- **Ne jamais ouvrir les pièces jointes ou cliquer sur des liens émanant de sources inconnues ;**
- **Accorder une attention particulière aux autorisations demandées par les applications ;**
- **Se méfier des annonces et comptes douteux sur les réseaux sociaux ;**
- **Bloquer, aux niveaux des solutions de sécurités, le trafic des utilisateurs vers les domaines compromis supra-cités ;**
- **Se conformer scrupuleusement au Référentiel National Normalisé de Sécurité Informatique.**